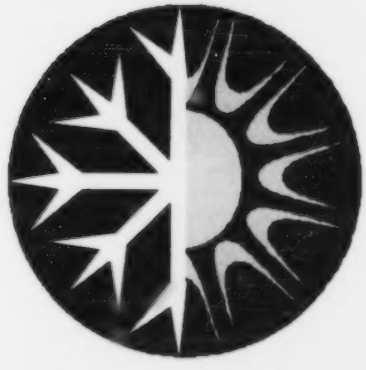
UNCLASSIFIED



Project SOLSTICE

Project SOLSTICE Report
Millennium Rollover Best Practices

Revision 6.0 25 October 1999

The objective of Project SOLSTICE is to prevent, detect, and respond to serious criminal activity which may target Canadian infrastructure during the Year 2000 transition. It is a multi-agency effort initiated by the Royal Canadian Mounted Police in co-operation with the Department of National Defence, Canadian Security Intelligence Service, Criminal Intelligence Canada, Canadian law enforcement and DOMUS Security Division LGS Group Inc.

Project SOLSTICE Report
Millennium Rollover Best Practices

Executive Summary

Many articles have been written about the potential and real problems that are associated with the Year 2000. By and large, most Canadian companies are aware of the potential disruption to their operations that date calculation errors may cause and have taken appropriate steps to correct critical applications before December 31st 1999. However, much work remains to be done and the risk of malfunction remains significant during the early part of year 2000.

If the information you process is critical to your ongoing business, your only choice is to repair or replace the application with one that can calculate the Year 2000 dates correctly. Unfortunately, the correction or replacement process used also created an opportunity for unethical programmers and others to create future paths into your IT environment they could use to attack your organization or its information. These access routes could allow them unchallenged access and the opportunity for illegal or criminal gain.

Many problems may not become apparent or occur in early January 2000. In addition, the rapid evolution of information technology environments may result in problems that are totally unrelated to Year 2000 but that will nevertheless disrupt your normal business processes. Management and Information Technology staff should guard against becoming complacent once the excitement of 1 January 2000 is over. Proper audits and assessments of all security and protection measures should be done before vigilance is relaxed.

Due-care precautions will ensure your organization will have an appropriate response to prevent and correct any type of problem whether they are Year 2000 related or not. The lists in the following pages are a reminder of best use practices you and your organization should follow to manage the remainder of your correction effort as well as the inevitable problems that will arise from those applications that may not be Year 2000 ready on December 31st 1999.

Project SOLSTICE Report
Millennium Rollover Best Practices

1. Introduction

Many articles have been written about the potential and real problems that are associated with the Year 2000. By and large, most Canadian companies are aware of the potential disruption to their operations these problems may cause and have taken appropriate steps to correct these issues before December 31st 1999. This note repeats many of the precautions and steps that may have already been taken, but are worth mentioning none the less.

Year 2000 problems are mainly programming problems that will affect how your business applications calculate dates. Special unique considerations for year 2000 changeover should have been programmed into the software/hardware/firmware that calculate dates for your applications. If they have not been programmed properly, these applications need to be reprogrammed and tested before December 31st, 1999.

As an organization, you are faced with two issues. First, were your applications programmed properly? If they were not, you can keep the status quo, replace the application with one that does the calculations properly or repair the current programs. Your choice will depend on the impact the failure of these applications will have on your business and the costs of making the appropriate changes. If the information being processed is critical to your ongoing business, your only choice is to repair or replace the application with one that can calculate the Year 2000 dates correctly.

The second issue is whether the application correction or replacement process has created the opportunity for other wrong doings against your organization or its information. These problems can come about in many ways. First, the correction practices may have allowed unauthorized changes to your application. As a result, your applications could fail due to a problem that is unrelated to a date miss-calculation. Secondly, unethical programmers may have programmed - unknown to you - access routes into your computing environment to allow them unchallenged access and the opportunity for illegal or criminal gain. Either of these problems may occur in normal development or maintenance work but the time pressures and the sheer volume of corrections that need to be done in view of the inevitability of the Year 2000 deadline means less testing might be done and thus more opportunity for wrong doing.

Unfortunately, as this note is being written in mid-October 1999, it is probably too late to take corrective measures if you have not already done so. However, the list below is a reminder of best use practices that should be followed to assist you in managing either the remainder of your correction effort or the inevitable problems from those applications that may not be Year 2000 ready on December 31st 1999.

Many problems may not become apparent or occur in early January 2000. Management and Information Technology staff should guard against becoming complacent within the first few months of year 2000. Proper assessments and audits of all security and protection measures should be done before vigilance is relaxed.

The rapid evolution of information technology environments will often result in problems that are totally unrelated to Year 2000. Normal "due-care" precautions will ensure appropriate responses are available to prevent and correct any type of problems that might occur immediately before or after 1 January 2000.

The measures below are grouped into 4 major categories: Prevention, Detection, Containment and Remediation.

1. Prevention measures are those that are used to prevent a future problem from occurring. For example, good operational procedures for installing a new application in a production environment reduce the likelihood that the new application will cause other existing applications to fail.
2. Detection measures are those that are used to notify the person responsible that a problem has occurred. As an example data integrity checks are used to verify that only valid data has been entered in an application.
3. Containment measures are those that limit the scope of any damage that might be done to your information-processing environment. Access controls based on user authentication are used to limit the program and data to which specific users have access.
4. Remediation measures are those that are used to correct a problem ***after*** it has occurred. A Contingency plan that outlines what to do to replace or repair a failed system component is one example of a remediation measure.

2. Prevention

1. Advise Management and staff against trying to access/test systems/applications to "see if they work" at and around midnight 31 December 1999 (this is also a good rule of thumb for phones, power, bank machines, etc.). Such curiosity might generate high usage that might in turn cause brownouts or adversely affect the availability of systems.
2. Ensure that new applications or initiatives that were being developed or worked on during the Year 2000 activities have been, or will be inspected to ensure that they have not been tampered with.
3. Review all vulnerabilities that have become exposed during the Year 2000 conversion process and ensure they have been addressed. Ensure that an IT Security person is involved in the review process.
4. Be cautious of strangers requesting access to systems, using Year 2000 inspections as a reason.
5. Caution staff against using e-mailed executables or attachments that are be distributed shortly before and after 1 January 2000, even if they come from "trusted" sources.
6. Advise employees that instructions from superiors that go against good business ethics should be reported to an appropriate authority (some company officials or Directors may find themselves in desperate positions and may succumb to these pressures by attempting desperate actions).
7. Encourage the use of Public Key Infrastructures or the use of reputable encryption with solid key management to ensure sensitive information remains in confidence or is not compromised with respect to its integrity.
8. Request that Network or System Administration staff monitor and clean-up user disk space allocations before and shortly after 1 January 2000.
9. If possible, change phone numbers to remote access points.

10. Verify that security clauses are in all existing contracts and ensure that the contractors are handling your data and systems in an appropriate fashion. Modify contracts where these clauses have not been included to reflect your information protection needs.
11. Verify that the firewall configuration and access rules have not been modified and are still effective.
12. Investigate unusual personnel-related changes within the enterprise (e.g., high staff turnover, changes in maintenance personnel, contractor turnover, changes in Internet Service Providers or other service providers, more frequent visits by sales staff, etc.).
13. Review the background check on the organizations that performed your Year 2000 conversion (assuming it wasn't done in-house), to see if there are any issues / actions pending against them (if they were dishonest with other companies they probably were with yours as well).
14. Review the background checks for all staff and contractors who would stand to benefit from Year 2000 mischief. Perform the checks for individuals who have worked on critical systems.
15. Perform Penetration Testing on all enterprise entry points.
16. Perform visual inspection of all critical and single points of failure within the enterprise shortly before 31 December 1999, focusing on suspicious or strange equipment or devices that don't belong.
17. Reclaim all sensitive information from Year 2000 Contractors.
18. Remove all non-essential access points to the enterprise, especially those that were initiated for Year 2000 conversion that are no longer required.
19. Perform an audit of access-cards and keys that where issued during Year 2000 mediation.
20. Retrieve as many access cards as possible from people (e.g., staff, contractors, students, partners, etc.) who no longer need them.
21. Review all physical security measures both before and after Jan. 1st to ensure that they are working properly (e.g., locks, alarms, access controls, etc.).
22. Revisit access-controls accounts to ensure that all accounts that should have been deleted after Year 2000 conversion have been deleted. Pay close attention to access privileges that were granted to sensitive facilities.
23. Scrutinize security of e-commerce applications and web-sites that were being developed at the same time that Year 2000 mediation was being conducted, if access (physical or logical) was possible.
24. Verify that all external (bridges, routers, VPNs, etc.) links that were installed to assist with Year 2000 purposes are reviewed and those that are no longer needed removed.
25. Verify that no new "unplanned" interfaces have been added as a result of Year 2000 activities.
26. Verify that NT server security configurations and profiles have not been adversely changed.
27. Verify that known security holes in web access paths have been checked and corrected with the appropriate program patches and corrections.
28. Inspect user ID and password files to ensure that no new unauthorized accounts have been added.
29. Verify that all suppliers of IT equipment and services are Year 2000 compliant. Ensure that critical components have been tested and shown to be fully operational.

30. Verify that all persons and/or organizations that are authorized to access your IT environment use Year 2000 compliant applications and equipment.
31. Maximize the use of Year 2000 compliant commercial software.
32. Ensure that all commercial software is up-to-date, and that all revision/patches have been properly installed and tested.
33. Ensure that the most current version of all Internet browsers is properly deployed throughout the enterprise.
34. Ensure staff are Year 2000 aware and that they understand the nature and impact of Year 2000 related events.

3. Detection

1. Audit access controls within critical applications or applications that handle sensitive information.
2. Advise employees to report activities of colleagues that are not in line with business ethics.
3. Ensure all appropriate firewall event logs are operational and that staff is available to analyze their content.
4. Verify that all copies of backups or other copies of information made during the year 2000 activities are accounted for. Investigate as required to locate all copies.
5. Look for lifestyle changes in employees during the months following January 2000, and investigate lavish increases in lifestyles.
6. Monitor email usage both inbound and outbound to the enterprise and question high usage or usage that involves large attachments.
7. Perform a comparison of user disk usage between 15 December 1999 and 15 January 2000, and investigate any significant increases.
8. Perform a Security Review / Audit within the January-June 2000 timeframe.
9. Review access logs for individuals accessing facilities at "strange" hours or in "odd" fashion (e.g., frequency of access, locations being accessed, etc.) as imposters may be using legitimate access privileges for evil purposes.
10. Review and monitor all security controls very closely from 1 January 2000 to March 31 1999 by performing regular tests and audits.
11. Review system and bandwidth usage in comparison with historical data to ensure that more traffic/database accesses are not occurring.
12. Verify that no unauthorized application accounts (ID/passwords) have been added.
13. Identify the cause of failure before deciding to disconnect systems.
14. High usage of networks and systems during the first few days of January 2000, especially email, may indicate unauthorized access to your environment. However, this higher than normal usage may also be people who connect with friends and colleagues around the world to obtain personal Year 2000 impact assessments and updates.

4. Containment

1. Appoint someone to monitor the security posture of the organization with respect to Year 2000 for seven (7) months starting December 1999 (this doesn't have to be a full-time position). This individual should be tasked with talking to staff and management and taking notes on anomalies and helping out with investigations.
2. Change **all** passwords for remote access points / technologies (e.g., PCAnyhere, CarbonCopy, routers with passwords, etc.) before mid-December.
3. Change as many passwords as possible and especially passwords to accounts with Administration, Supervisor and/or Super-User privileges before the end of December.
4. Change as many cipher lock combinations as possible before the end of December.
5. Delete all unnecessary application accounts.
6. Verify that available Intrusion Detection Systems and/or procedures are operational and functioning properly.
7. Turn off as many non-essential systems that have not been converted as possible during the transition period (31 December 1999 to 1 January 2000).

5. Remediation

1. An assessment should be done to consider operating your enterprise from a contingency position (i.e., using backup generators and systems) from 22:00 on 31 December 1999 to 10:00 1 January 2000, to avoid power and telecommunication brownouts that will be caused as a high volumes of curious people "experiment" to see what works and what doesn't.
2. Be aware that not all problems that occur around 1 January 2000 will be caused by Year 2000. In some cases these problems may actually be planned attacks that are unrelated to Year 2000. All incidents should be investigated to determine their exact cause(s).
3. Ensure that batteries on Uninterrupted Power Supplies (UPSs) are fully charged and fuel tanks for backup power systems are full.
4. Ensure that system and data backups have been performed and that the backups have been validated and verified complete and accurate.
5. Ensure virus-checking software is up-to-date and properly deployed and installed. Ensure the virus checking software used verifies both virus signatures and improper system accesses. Implement a proactive response plan if new or previously unknown types of viruses appear.
6. Inform management and staff that problems which occur after 1 January 2000 will not naturally be assumed to be Year 2000 related (note: this may discourage Management and staff from hatching schemes and blaming results if caught, on Year 2000 issues).
7. Remember, just because you don't see a problem doesn't mean that they aren't there.
8. Review the frequency of backups during the 15 December to 15 January time period. Additional backups taken during the day might be warranted based on the stability of the information technology within the enterprise.
9. Verify that backups needed for contingency and recovery plans work properly after 1 January 2000.

6. Contact Information

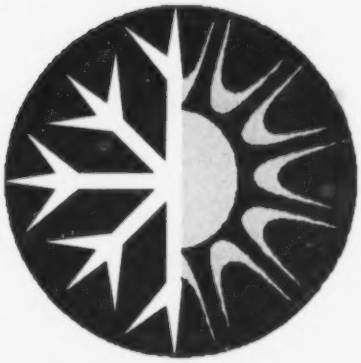
For additional information regarding Project SOLSTICE, or requests for future revisions of this document, please contact:

C. R. (Chuck) Waring
Project Manager, Project SOLSTICE
Criminal Intelligence Directorate
Royal Canadian Mounted Police
1200 Vanier Parkway
Ottawa, Ontario Canada
K1A 0R2
Telephone: 613-993-2166
Facsimile: 613-993-9668

For additional information concerning the best practices contained in this document, or suggestions for future revisions, please contact:

Daniel Morrison
Practice Leader and Senior Director
DOMUS Security Practice
LGS Group Inc.
309 Cooper Street, Suite 200
Ottawa, Ontario Canada
K2P 0G5
Phone: 613 230 6285 ext 304
Facsimile: 613 230 3274
email: dan_morrison@lgs.com

NON CLASSIFIÉ



Projet SOLSTICE

Rapport sur le projet SOLSTICE
Meilleures pratiques en vue du passage à l'an 2000

Révision 6.0 25 octobre 1999

Le projet SOLSTICE vise à prévenir, à détecter et à contrer toute activité criminelle susceptible de cibler les infrastructures canadiennes au moment du passage à l'an 2000. Il s'agit d'un effort concerté lancé à l'initiative de la Gendarmerie royale du Canada en collaboration avec le ministère de la Défense, le Service canadien du renseignement de sécurité, le Service canadien de renseignements criminels, la police canadienne et la division sécurité de DOMUS-LGS Group Inc.

NON CLASSIFIÉ

Rapport sur le projet SOLSTICE
Meilleures pratiques en vue du passage à l'an 2000

Sommaire

De nombreux articles ont été consacrés aux problèmes réels et potentiels liés au passage à l'an 2000. De manière générale, la plupart des entreprises canadiennes sont conscientes des perturbations que des erreurs dans le calcul de la date pourraient causer à leurs activités et ont pris les mesures qui s'imposent afin de corriger leurs applications essentielles avant le 31 décembre 1999. Cependant, il reste beaucoup à faire et le risque que des dysfonctionnements se produisent au début de l'année 2000 demeure encore élevé.

Si l'information que vous traitez est essentielle à vos activités courantes, vous n'avez d'autre choix que de remplacer ou de corriger vos applications pour qu'elles calculent correctement les dates de l'an 2000. Hélas, des programmeurs ou autres personnages peu scrupuleux pourraient profiter de ce processus de correction et de remplacement des applications pour pratiquer discrètement des chemins d'accès dans votre environnement TI, dont ils se serviront ensuite pour attaquer votre organisation ou son information. Ils pourraient utiliser ces chemins à votre insu pour réaliser des profits criminels ou illégaux.

De nombreux problèmes pourraient ne pas se manifester dès le début du mois de janvier 2000. En outre, l'évolution rapide des environnements TI pourrait entraîner des problèmes qui n'ont rien à voir avec le bogue de l'an 2000, mais qui n'en perturberont pas moins vos processus opérationnels. Le personnel TI et de gestion devra se garder de toute complaisance une fois le 1er janvier 2000 passé. Il faudra dûment évaluer et vérifier toutes les mesures de protection et de sécurité avant de relâcher un tant soit peu sa vigilance.

En prenant les précautions nécessaires, vous vous assurerez que votre organisation sera en mesure de prévenir et de corriger tout problème, qu'il soit relié ou non au bogue de l'an 2000. Vous trouverez ci-joint une liste des meilleures pratiques que nous vous recommandons d'appliquer au reste de vos efforts de correction, ainsi qu'une description des inévitables problèmes que provoqueront les applications qui n'auront pas été mises en conformité au 31 décembre 1999.

1. Introduction

De nombreux articles ont été consacrés aux problèmes réels et potentiels liés au passage à l'an 2000. De manière générale, la plupart des entreprises canadiennes sont conscientes des perturbations que des erreurs dans le calcul de la date pourraient causer à leurs activités et ont pris les mesures qui s'imposent afin de corriger leurs applications essentielles avant le 31 décembre 1999. Le présent document constitue un rappel de ces précautions et mesures qui, même si elles ont déjà été prises, n'en sont pas moins utiles à mentionner.

Le bogue de l'an 2000 renvoie principalement aux erreurs de programmation qui affecteront la manière dont vos applications de gestion caculeront les dates. Les logiciels, matériels et microprogrammes qui calculent les dates pour vos applications devraient avoir fait l'objet d'une programmation particulière en vue du passage à l'an 2000. S'ils n'ont pas été correctement programmés, ils devront être modifiés, puis testés avant le 31 décembre 1999.

En tant qu'organisation, vous devez vous poser deux questions : D'abord, vos applications ont-elles été correctement programmées? Dans la négative, vous avez le choix entre le statu quo, remplacer l'application par une autre qui effectue correctement les calculs, ou encore corriger les programmes existants. Votre décision dépendra de l'incidence qu'aurait une panne de ces applications sur vos activités et de ce qu'il vous en coûterait pour effectuer les changements nécessaires. Si l'information que vous traitez est essentielle à vos activités courantes, vous n'avez d'autre choix que de remplacer ou de corriger vos applications pour qu'elles calculent correctement les dates de l'an 2000.

Ensuite, vous devez vous poser la question de savoir si ce processus de remplacement ou de correction des applications n'a pas servi de prétexte à des actions visant à nuire à l'intégrité de votre organisation ou de son information. Les exemples sont nombreux. D'abord, on pourrait avoir profité des travaux de correction pour modifier vos applications sans votre consentement. Celles-ci pourraient ainsi cesser de fonctionner pour des raisons qui n'ont rien à voir avec une erreur de calcul de la date. Ensuite, des programmeurs déloyaux pourraient avoir programmé - à votre insu - des chemins d'accès dans votre environnement informatique qu'ils pourront ensuite emprunter sans être repérés, ce qui leur permettra de réaliser des profits criminels ou illégaux. Certes, tout cela peut aussi bien se produire dans le cours normal des travaux de maintenance ou de conception, mais les contraintes de temps et l'important volume de corrections rendues nécessaires par la date fatidique du 1er janvier 2000 pourraient pousser à escamoter certains tests, créant ainsi une situation particulièrement favorable à la perpétration de certains méfaits.

À l'heure où nous rédigeons ces lignes, soit à la mi-octobre 1999, il est sans doute trop tard pour prendre des mesures correctives. Vous trouverez néanmoins ci-joint une liste des meilleures pratiques qui devraient vous aider, selon le cas, à organiser la suite de vos efforts de correction ou à gérer les inévitables problèmes qu'engendreront les applications qui n'auront pas été mises en conformité à l'an 2000 le 31 décembre 1999.

De nombreux problèmes pourraient ne pas se manifester dès le début du mois de janvier 2000. Le personnel TI et de gestion devra se garder de toute complaisance durant les premiers mois de l'an 2000. Il faudra dûment évaluer et vérifier toutes les mesures de protection et de sécurité avant de relâcher un tant soit peu sa vigilance.

L'évolution rapide des environnements TI provoquera des problèmes qui n'auront souvent rien à voir avec le bogue de l'an 2000. En prenant les précautions nécessaires, vous disposerez d'un

processus d'intervention approprié pour prévenir et corriger tout problème qui pourrait survenir immédiatement avant ou après le 1er janvier 2000.

Les mesures ci-dessous sont réparties en quatre grandes catégories : la prévention, la détection, l'endiguement et la correction.

1. Les mesures préventives visent à éviter l'apparition d'un problème. Ainsi, si on installe une nouvelle application en suivant des procédures opérationnelles efficaces, on réduit le risque de voir les applications existantes tomber en panne.
2. Les mesures de détection visent à détecter un problème et à le signaler à la personne responsable. À titre d'exemple, les contrôles d'intégrité des données permettent de vérifier que seules les données valides ont été saisies dans une application.
3. Les mesures d'endiguement visent à limiter l'ampleur des dommages susceptibles d'être causés à votre environnement de traitement de l'information. Les contrôles d'accès basés sur l'authentification de l'usager servent à limiter les données et les programmes auxquels chaque usager a accès.
4. Les mesures correctives visent à corriger un problème ***après coup***. On peut citer comme exemple les plans d'urgence qui indiquent comment réparer ou remplacer tel élément d'un système en panne.

2. Mesures préventives

1. Recommander au personnel et à la direction de ne pas tenter d'entrer dans les applications et systèmes, ni de les tester « pour voir s'ils fonctionnent » aux alentours du 31 décembre 1999 à minuit (le conseil vaut également pour les téléphones, le courant, le matériel bancaire, etc.). Cela risquerait de saturer les systèmes, causant en retour des pannes de courant localisées ou affectant la disponibilité des systèmes.
2. Vérifier l'intégrité de toutes les nouvelles applications ou initiatives lancées ou élaborées durant les travaux de conformité à l'an 2000.
3. Revoir toutes les vulnérabilités mises au jour par le processus de mise en conformité à l'an 2000 et s'assurer qu'elles ont été corrigées. Veiller à ce qu'un employé de la sécurité des TI participe à l'exercice.
4. Se méfier des inconnus qui sollicitent l'accès aux systèmes en prétendant vérifier leur conformité à l'an 2000.
5. Demander au personnel de ne pas ouvrir les pièces jointes ou exécutables transmis par courrier électronique peu avant ou après le 1er janvier 2000, même s'ils proviennent de sources « fiables ».
6. Recommander aux employés de rapporter à une autorité compétente toute instruction de leurs supérieurs qui serait contraire à la déontologie (certains responsables ou directeurs d'entreprise acculés pourraient succomber à la tentation d'entreprendre des actions desespérées).
7. Promouvoir l'utilisation de l'infrastructure à clés publiques ou de toute autre méthode de cryptage reconnue basée sur une gestion des clés rigoureuse afin de préserver la confidentialité et l'intégrité de l'information.

8. Demander au personnel de l'administration du système ou du réseau de vérifier et de nettoyer les espaces disque alloués aux usagers avant et peu après le 1er janvier 2000.
9. Dans la mesure du possible, modifier les numéros de téléphone des points d'accès à distance.
10. Vérifier l'existence de clauses de sécurité dans tous les contrats et s'assurer que tous les entrepreneurs traitent vos données et systèmes comme il se doit. S'il y a lieu, insérer des clauses de sécurité reflétant vos exigences en matière de protection de l'information.
11. Vérifier l'intégrité et la validité des règles d'accès et de la configuration du garde-barrière.
12. Enquêter sur tout changement inhabituel dans le personnel de l'entreprise (par ex. roulement élevé de personnel, changements de personnel de maintenance, rotation d'entrepreneurs, changements de fournisseurs d'accès Internet ou autres fournisseurs de services, visites plus fréquentes du personnel de vente, etc.).
13. Vérifier les antécédents/références des entreprises qui ont effectué vos travaux de conformité à l'an 2000 (s'ils n'ont pas été réalisés à l'interne) afin de cerner tout problème/action prise à leur encontre (si elles ont été malhonnêtes avec d'autres compagnies, elles l'ont sans doute été avec vous).
14. Vérifier les antécédents/références du personnel et des entrepreneurs qui pourraient avoir avantage à commettre un méfait en prévision du passage à l'an 2000. Vérifier les antécédents des personnes qui ont travaillé sur les systèmes essentiels.
15. Effectuer des tests de pénétration sur tous les points d'entrée.
16. Peu avant le 31 décembre 1999, inspecter visuellement tous les points de panne unique dans l'entreprise en portant une attention particulière aux équipements ou dispositifs étranges, suspects ou inconnus.
17. Récupérer toute l'information sensible auprès des entrepreneurs chargés des travaux de conformité à l'an 2000.
18. Supprimer tous les points d'accès à l'entreprise qui ne sont pas indispensables, notamment ceux qui ont été installés en prévision des travaux de conformité à l'an 2000 et qui n'ont plus lieu d'être.
19. Vérifier les cartes-clés et les clés de protection émises durant les travaux de conformité à l'an 2000.
20. Récupérer le maximum de cartes-clés des personnes qui n'en ont plus besoin (personnel, entrepreneurs, étudiants, partenaires, etc.).
21. Vérifier le fonctionnement des dispositifs de sécurité physique avant et après le 1er janvier 2000 (verrous, alarmes, contrôles d'accès, etc.).
22. Revoir les registres de contrôle d'accès pour s'assurer que tous les comptes qui auraient dû être supprimés après les travaux de mise en conformité à l'an 2000 ont bien été effacés. Examiner attentivement les privilèges d'accès aux installations sensibles.
23. Vérifier attentivement la sécurité des sites Web et applications de commerce électronique conçus pendant les travaux de conformité à l'an 2000, si un accès (physique ou logique) était possible.
24. Examiner tous les liens externes (passerelles, routeurs, RPV, etc.) installés pour faciliter les travaux de conformité à l'an 2000 et supprimer ceux qui ne sont plus nécessaires.
25. S'assurer qu'on n'a ajouté aucune nouvelle interface « imprévue » dans la foulée des travaux de conformité à l'an 2000.

26. Vérifier que les configurations et profils de la sécurité du serveur de réseau n'ont pas été indûment modifiés.
27. S'assurer que les trous de sécurité pratiqués dans les chemins d'accès au Web ont été vérifiés et corrigés au moyen de corrections de programme adéquates.
28. Examiner les fichiers de mots de passe et d'ID utilisateurs pour s'assurer qu'aucun compte non autorisé n'a été ajouté.
29. Vérifier la conformité à l'an 2000 des fournisseurs de services et de matériel TI. S'assurer que toutes les composantes essentielles ont été testées et validées.
30. S'assurer que toutes les personnes et organisations autorisées à pénétrer dans votre environnement TI utilisent des applications et du matériel conformes à l'an 2000.
31. Optimiser l'utilisation du progiciel commercial de mise en conformité à l'an 2000.
32. S'assurer que tous les progiciels commerciaux sont à jour et que toutes les révisions/corrections ont été correctement installées et testées.
33. Veiller à ce que la dernière version des fureteurs soit installée dans toute l'entreprise.
34. S'assurer que le personnel est conscient des enjeux liés au bogue de l'an 2000 et qu'il comprend la nature et l'impact des risques qui y sont associés.

3. Mesures de détection

1. Vérifier les contrôles d'accès aux applications essentielles ou à celles qui traitent ou contiennent de l'information sensible.
2. Recommander aux employés de dénoncer les activités de leurs collègues qui dérogent à la déontologie.
3. S'assurer que tous les registres du garde-barrière sont opérationnels et que du personnel est disponible pour en analyser le contenu.
4. Vérifier que toutes les copies de sauvegarde et autres copies de données effectuées durant les travaux de conformité à l'an 2000 sont localisées. S'il y a lieu, rechercher les copies manquantes.
5. Rester à l'affût de tout changement dans le train de vie des employés durant les premiers mois de l'an 2000 et enquêter sur toute hausse subite et importante de leur style de vie.
6. Contrôler l'utilisation du courrier électronique de l'entreprise à l'arrivée comme au départ et s'interroger sur tout usage excessif ou transmission de pièces jointes volumineuses.
7. Comparer l'utilisation du disque de l'usager entre le 15 décembre 1999 et le 15 janvier 2000 et enquêter sur toute hausse inhabituelle.
8. Effectuer un examen/vérification de la sécurité pour la période de janvier à juin 2000.
9. Examiner les registres d'accès des personnes qui pénètrent dans les installations à des heures « étranges » ou de manière « inusitée » (fréquence d'accès, endroits pénétrés, etc.); des imposteurs pourraient utiliser des privilèges d'accès légitimes à des fins malveillantes.
10. Surveiller attentivement les contrôles de sécurité du 1er janvier au 31 mars 2000 en effectuant des vérifications et des tests à intervalles réguliers.
11. Comparer l'utilisation du système et de la bande passante avec les données historiques afin de détecter toute hausse de trafic ou d'accès aux bases de données.

12. Vérifier qu'aucun compte non autorisé (ID/mots de passe) n'a été ajouté aux applications.
13. Déterminer l'origine de la panne avant de décider s'il faut débrancher les systèmes.
14. Une utilisation élevée des réseaux et des systèmes durant les premiers jours de janvier 2000, notamment du courrier électronique, pourrait être l'indice d'un accès non autorisé à votre environnement. Cependant, il se pourrait aussi que des personnes communiquent avec des amis ou collègues de par le monde pour recueillir leurs impressions sur le passage à l'an 2000, suscitant par le fait même un usage plus élevé que la normale.

4. Mesures d'endiguement

1. Charger une personne de contrôler le niveau de sécurité de l'organisation en regard du problème de l'an 2000 sur une période de sept mois à compter de décembre 1999 (pas nécessairement à temps plein). La personne choisie discutera avec le personnel et la direction, prendra note des anomalies relevées et aidera aux enquêtes.
2. Modifier **tous** les mots de passe des points d'accès/technologie à distance (PCAnyhere, CarbonCopy, routeurs avec mots de passe, etc.) avant la mi-décembre.
3. Modifier le maximum de mots de passe, notamment pour les comptes avec privilèges d'administration, de superviseur ou de super-utilisateur, avant la fin décembre.
4. Modifier le maximum de combinaisons chiffrées des verrous avant la fin décembre.
5. Supprimer tous les comptes inutiles.
6. Vérifier que des procédures ou systèmes de détection d'intrusion sont en place et qu'ils fonctionnent normalement.
7. Débrancher le maximum de systèmes secondaires non conformes du 31 décembre 1999 au 1er janvier 2000.

5. Mesures correctives

1. Évaluer l'opportunité pour votre entreprise de fonctionner en mode d'urgence (c'est-à-dire en s'appuyant sur des systèmes et des génératrices de secours) du 31 décembre 1999 à 22 h au 1er janvier 2000 à 10 h pour éviter les pannes de courant et de télécommunications localisées qui ne manqueront pas de se produire si une foule de curieux décide de « voir » ce qui fonctionne ou pas.
2. Ne pas oublier que les problèmes qui se produiront aux alentours du 1er janvier 2000 ne seront pas tous causés par le bogue de l'an 2000. Dans certains cas, il pourrait s'agir d'attaques planifiées qui n'ont rien à voir avec le bogue. Il faudra enquêter sur chaque incident pour en déterminer la cause exacte.
3. Vérifier le chargement des batteries des systèmes d'alimentation électrique sans interruption (systèmes SI) et le plein des réservoirs à essence qui alimenteront les génératrices de secours.
4. Vérifier que des copies de sauvegarde des données et des systèmes ont été effectuées et que leur contenu a été vérifié et validé comme étant complet et exact.

5. S'assurer que les logiciels de détection de virus sont à jour et qu'ils sont correctement installés et activés. Vérifier que le logiciel antivirus utilisé vérifie et la signature de virus, et les accès abusifs au système. Mettre en place un plan d'intervention proactif en prévision de l'apparition de virus inconnus ou nouveaux.
6. Prévenir le personnel et les gestionnaires que les problèmes qui pourraient surgir après le 1er janvier 2000 ne seront pas mis systématiquement sur le compte du problème de l'an 2000 (cela devrait dissuader les mauvais esprits de profiter du problème de l'an 2000 pour comploter quelque machination).
7. Garder à l'esprit qu'il peut y avoir un problème même si on ne le voit pas.
8. Revoir la fréquence des sauvegardes du 15 décembre 1999 au 15 janvier 2000. Selon la stabilité de la technologie de l'information dans l'entreprise, il pourrait être nécessaire d'effectuer des sauvegardes additionnelles durant la journée.
9. Vérifier que les copies de sauvegarde nécessaires aux plans d'urgence et de reprise des opérations fonctionnement normalement après le 1er janvier 2000.

6. Personnes-ressources

Pour de plus amples renseignements sur le projet SOLSTICE ou pour obtenir un exemplaire des futures mises à jour du présent document, communiquez avec :

C. R. (Chuck) Waring
gestionnaire du Projet SOLSTICE
Direction des renseignements criminels
Gendarmerie royale du Canada
1200, promenade Vanier
Ottawa (Ontario) Canada
K1A 0R2
Téléphone : (613) 993-2166
Télécopieur : (613) 993-9668

Pour de plus amples renseignements sur les meilleures pratiques susmentionnées ou pour formuler des suggestions en vue des prochaines mises à jour du présent document communiquez avec :

Daniel Morrison
directeur principal et chef des pratiques en matière de sécurité
DOMUS Security Practice
LGS Group Inc.
309, rue Cooper, bureau 200
Ottawa (Ontario) Canada
K2P 0G5
Téléphone : (613) 230-6285, poste 304
Télécopieur : (613) 230-3274
Adresse électronique : *dan_morrison@lgs.com*